BOREUS
rechenzentrum gmbh

Post-Quanten-Kryptographie
Wie sieht die Zukunft der Verschlüsselung aus?

Paul Brüdgam (Boreus Rechenzentrum GmbH)

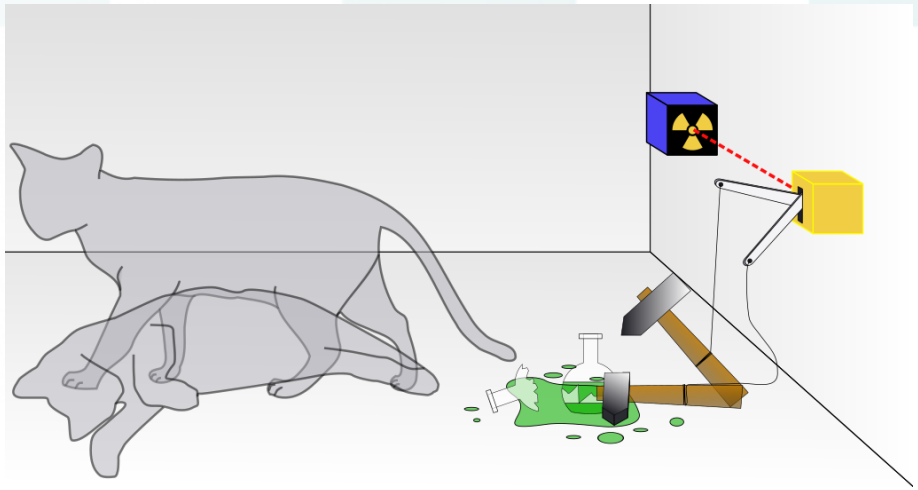
Zu meiner Person

- Bachelor in Informations- und Kommunikationstechnik (FH Stralsund)
- Master in Wirtschaftsinformatik (FH Stralsund)
  - Abschlussthema: Post-Quanten-Kryptographie – Motivation & praktische Anwendung
- Mitarbeiter der Boreus Rechenzentrum GmbH

Motivation und Ziele

- „Quantencomputer stellen eine Gefahr für moderne Kryptographie dar“
- Warum sind sie eine Gefahr?
- Post-Quanten-Kryptographie (PQC)?
- Wie leistungsfähig sind mögliche PQC-Verfahren?
- Was bedeuten Quanten Computing und PQC-Verfahren für heutige Rechnernetze?

BOREUS
rechenzentrum gmbh



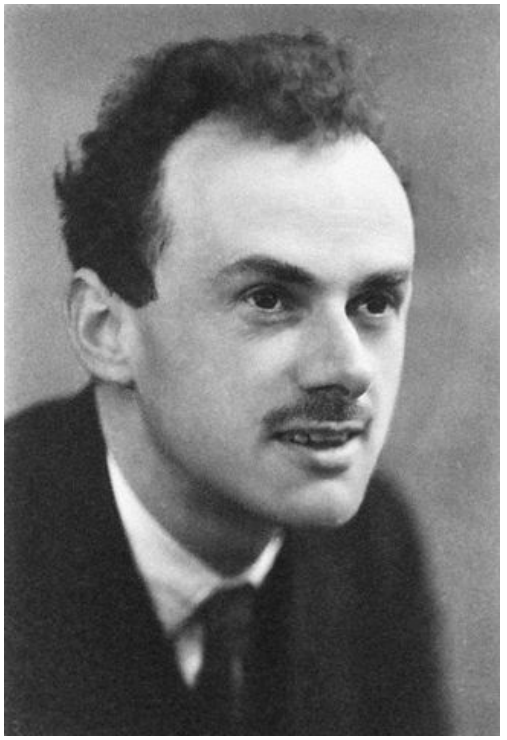
Quantum Computing

Willkommen in einer surrealen Welt

Begriffe

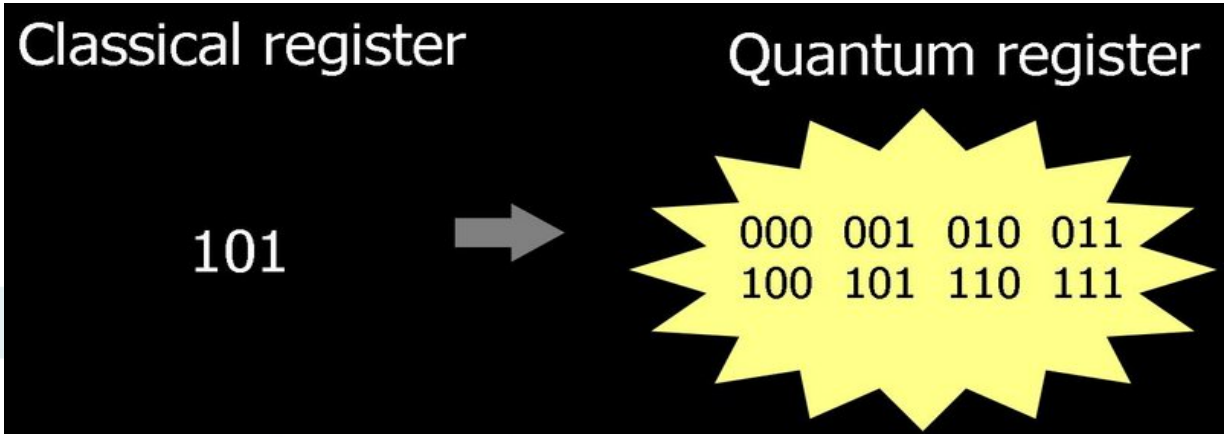
Quantum Computing - Begriffe

- Bracket-Notation (Dirac-Notation)
  - eingeführte Schreibart für die Vektoren n
    - des abstrakten quanten-mechanischen Hilbert-Raumes H (Ket-Vektoren $|n\rangle$)
    - des zugeordneten Dualraumes H* (Bra-Vektoren $\langle n|$)



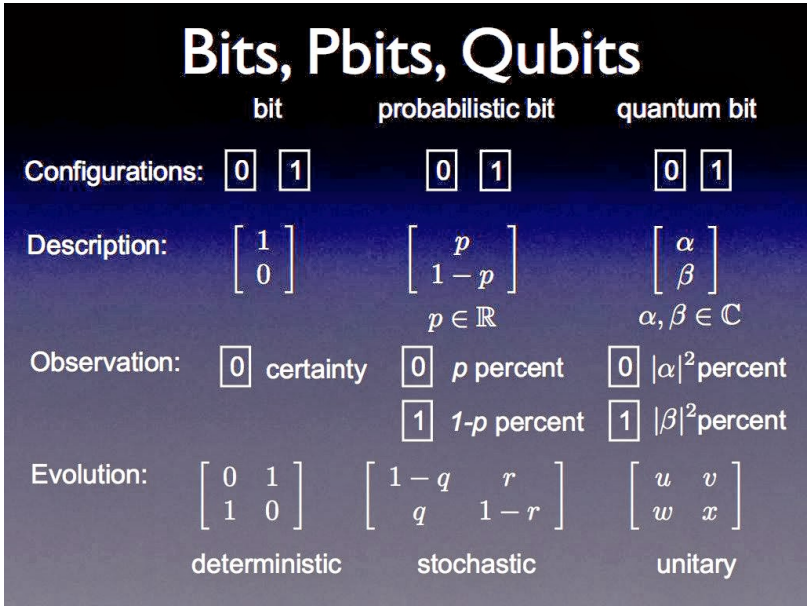
Quantum Computing - Begriffe

- Superposition (Quantenphysik)
  - Anwendung auf abgeschottete Atome / kleine Teilchen (z.B. Photonen)
  - Überlagerung mehrerer Zustände
  - Zerstörung der Superposition durch Messen



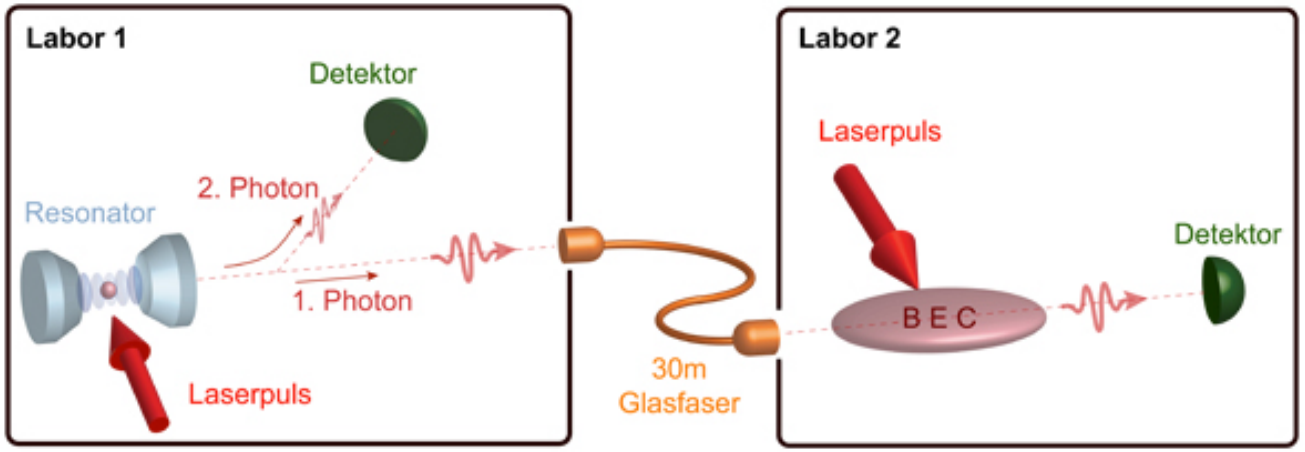
Quantum Computing - Begriffe

- Quantenbit
  - Form: $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ mit $\alpha, \beta \in \mathbb{C}$ und $|\alpha|^2 + |\beta|^2 = 1$
  - Superposition muss gemessen werden, um Wahrscheinlichkeit eines Zustandes zu erfahren
  - können klassische Bits darstellen



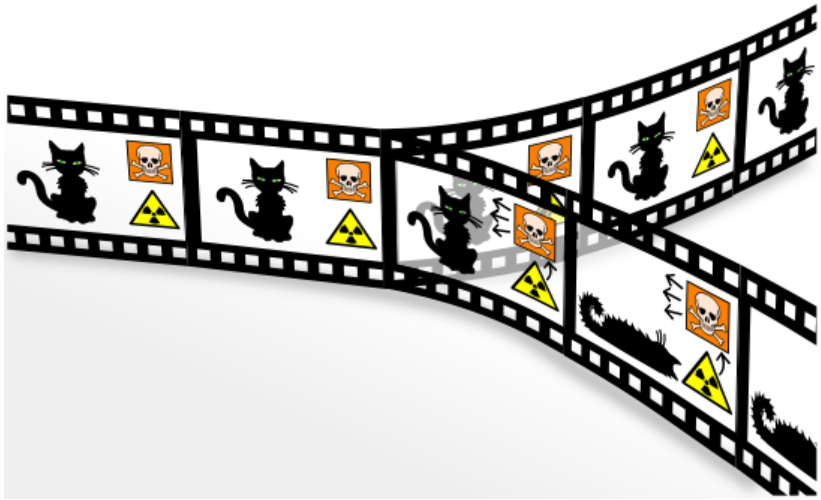
Quantum Computing - Begriffe

- Verschränkung
  - Quantenbits sind auf „bestimmte Weise“ verbunden
  - Quantenbits behalten ihren Zustand auch bei Trennung, solange sie isoliert von ihrer Umwelt sind
  - Wird ein Quantenbit gemessen, dann hat das andere den selben Zustand



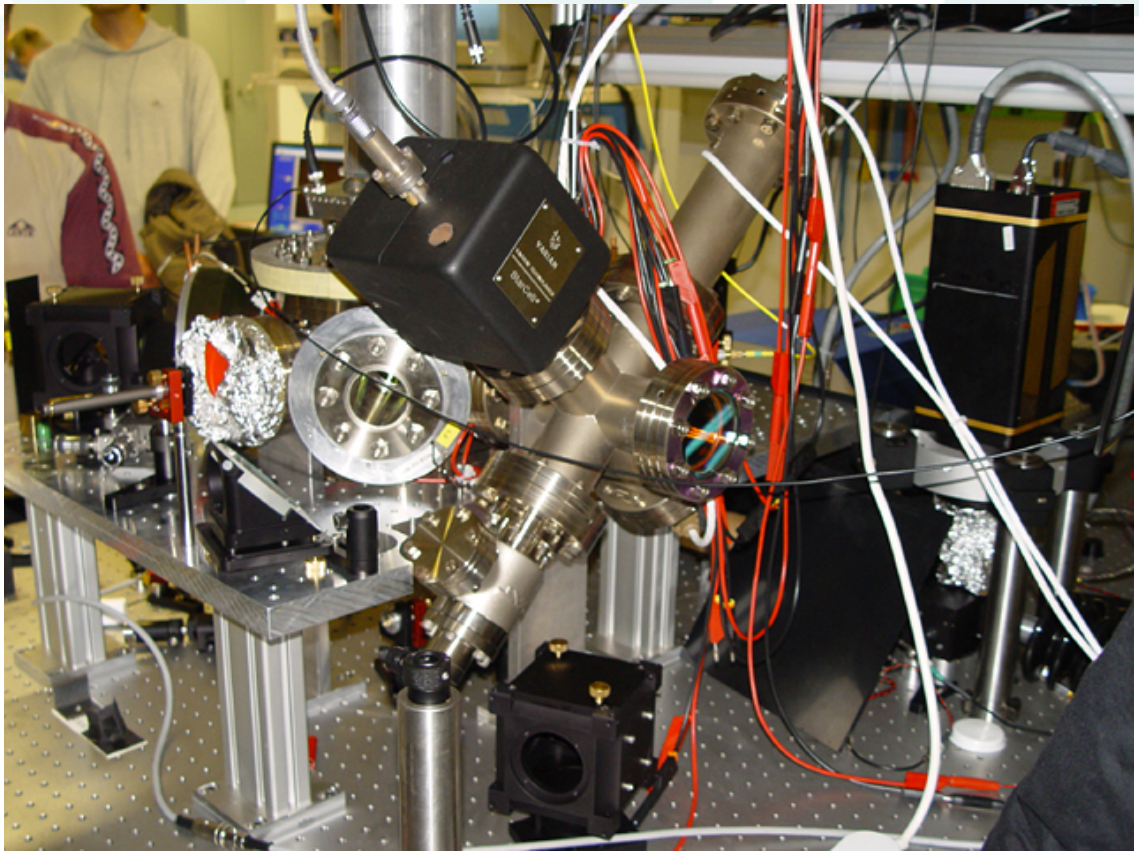
Quantum Computing - Begriffe

- Dekohärenz
  - Wechselwirkung von Quantenzuständen mit der Umgebung
  - Quantenbits lassen sich nicht perfekt abschirmen
  - Bestimmt Anzahl der Transformationen
  - Am Beispiel der Katze nimmt die Außenwelt den Zustand der Katze an, wenn sich die Kiste öffnet (Informationstrennung unmöglich)



Quantum Computing

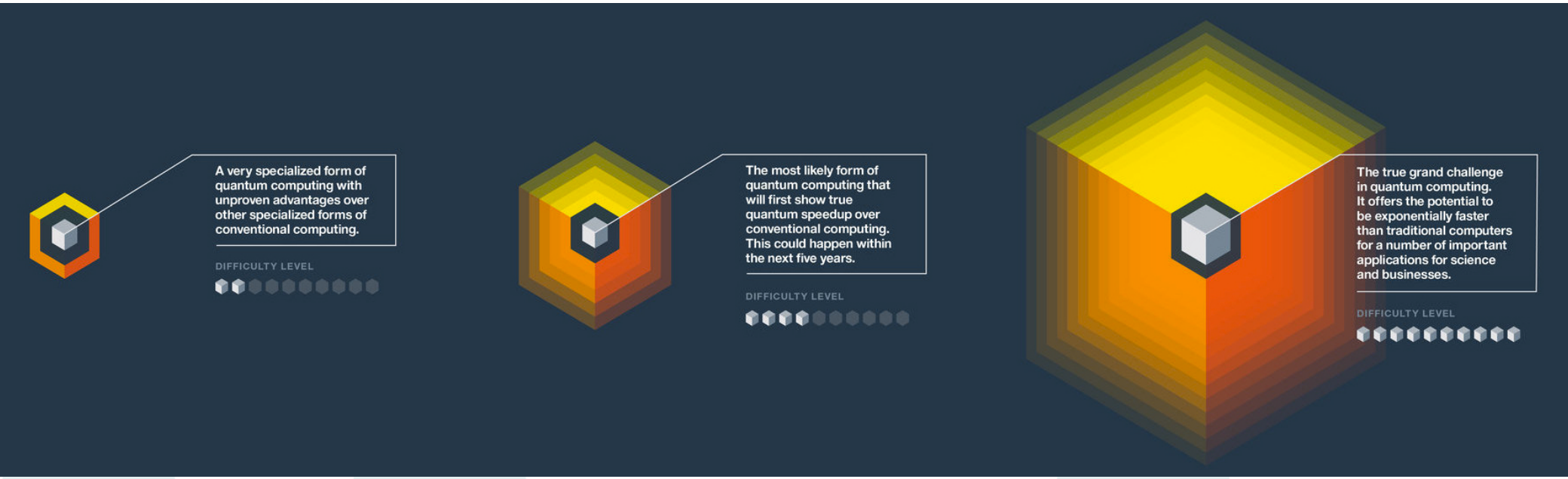
Arten



BOREUS
rechenzentrum gmbh

Quantum Computing - Arten

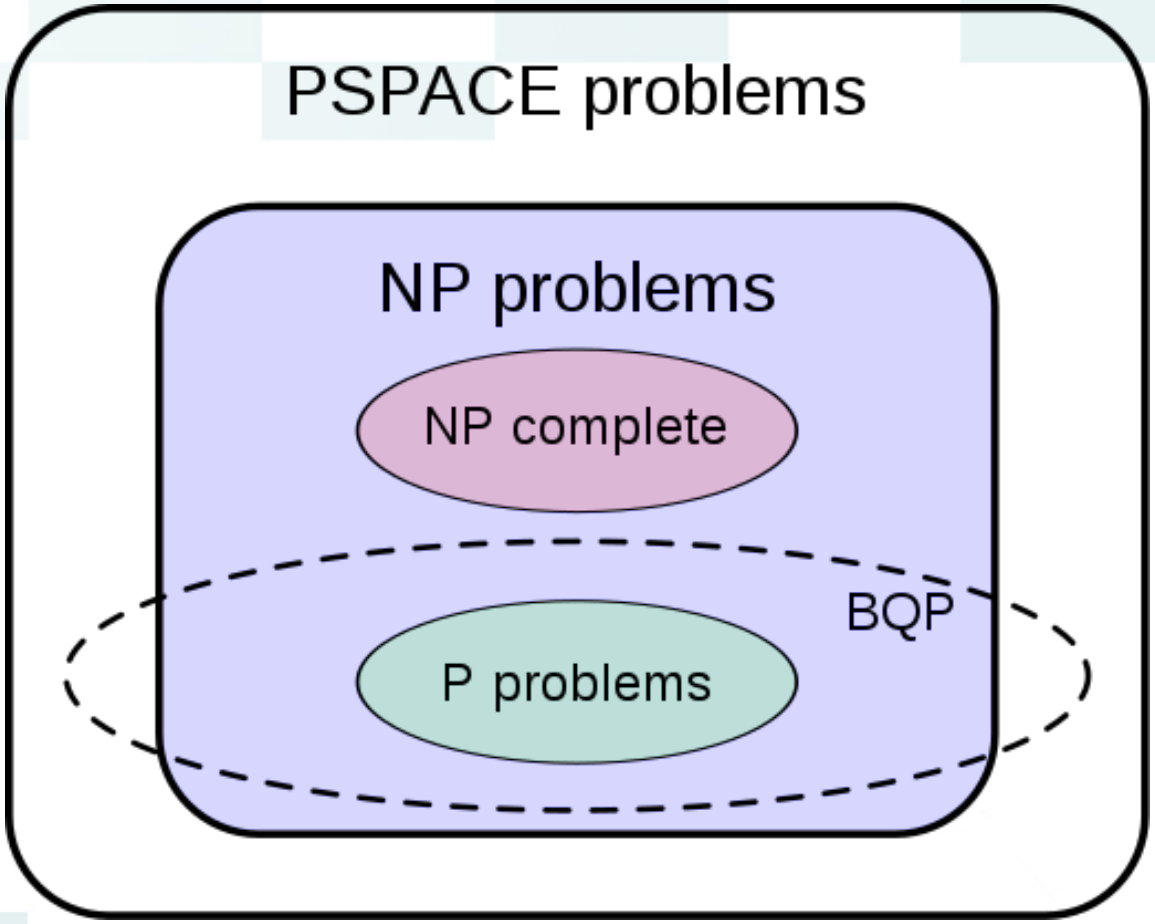
- Quantenanealer
- Analoger Quantencomputer
- Universeller Quantencomputer



Quantum Computing - Arten

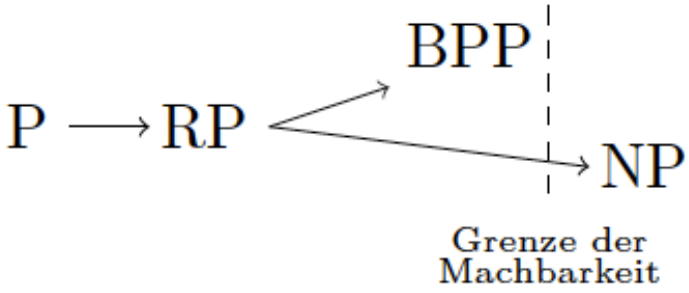
Art/Generality	Anwendung	Allgemeine Informationen
Quantenanealer (restriktiv)	Optimierungsprobleme	• Einfach zu bauen • Kann eine bestimmte Funktion ausführen • Keine Leistungsvorteile
Analoger Quantencomputer (teilweise)	Quantenchemie Materialwissenschaft Sampling Quanten-Dynamik	• Kann komplexe Simulationen ausführen • 50 bis 100 Qubits • Hohe Leistung
Universeller Quantencomputer (vollkommen)	Machine Learning Kryptographie Suche Secure Computing	• >100.000 Qubits • Extrem hohe Leistung • Kann nicht alle Probleme effizient lösen

Algorithmen



Quantum Computing - Algorithmen

- Quantenalgorithmen sind probabilistische Algorithmen
  - ermöglichen eine Fehlerreduzierung bei mehrfacher Wiederholung
- Komplexitätsklassen BQP, BQNP
- Bekannte Algorithmen:
  - Algorithmus von Shor
  - Algorithmus von Grover
  - Algorithmus von Deutsch (Verallgemeinerung Deutsch-Josza-Algorithmus)



Quantum Computing - Algorithmen

- Algorithmus von Shor
  - Polynomialzeit-Algorithmus für die Faktorisierung und das Diskrete-Logarithmus-Problem (DLP)
  - Idee: Faktorisierung lässt sich auf die Bestimmung der Periode von a mod n, kleinstes r mit a^r mod n = 1, zurückführen
  - Klassischer Teil zur Problemreduzierung und Quantenteil zur effizienten Lösung des Restproblems (Bestimme die Ordnung r von $f(a) = x^a \bmod n$)
  - Es werden $\mathcal{O}(\log \log r)$ Wiederholungen benötigt, um mit hoher Wahrscheinlichkeit r zu finden.

Quantum Computing - Algorithmen

- Algorithmus von Grover
  - Polynomialzeit-Algorithmus für die Suche in **unsortierten** Datenbanken mit N Einträgen [N = 100000]
  - Klassische Computer benötigen eine Laufzeit von
    - $\mathcal{O}(N)$ (lineare Suche) [100000]
    - $\mathcal{O}(\log(\log(N)))$ binäre Suche/Interpolationssuche für **sortierte** Datenbanken
  - Quantencomputer benötigen eine Laufzeit von $\mathcal{O}(\sqrt{N})$ [316]
  - Für Optimierungsprobleme der Komplexitätsklasse NP
  - Eignet sich für das Durchsuchen von Schlüsselräumen

BOREUS
rechenzentrum gmbh

Auswirkungen von Quantum Computing

Impact für heutige Kryptographie?

Quantum Computing - Auswirkungen

Überblick der heutigen Krypto-Landschaft

- Asymmetrische Kryptographie
  - Diffie-Hellman, RSA, ElGamal (DSA), ECC (ECDH, ECDSA)
- Symmetrische Kryptographie
  - DES, AES
- Kryptographische Hashfunktionen
  - SHA1, SHA2, SHA3

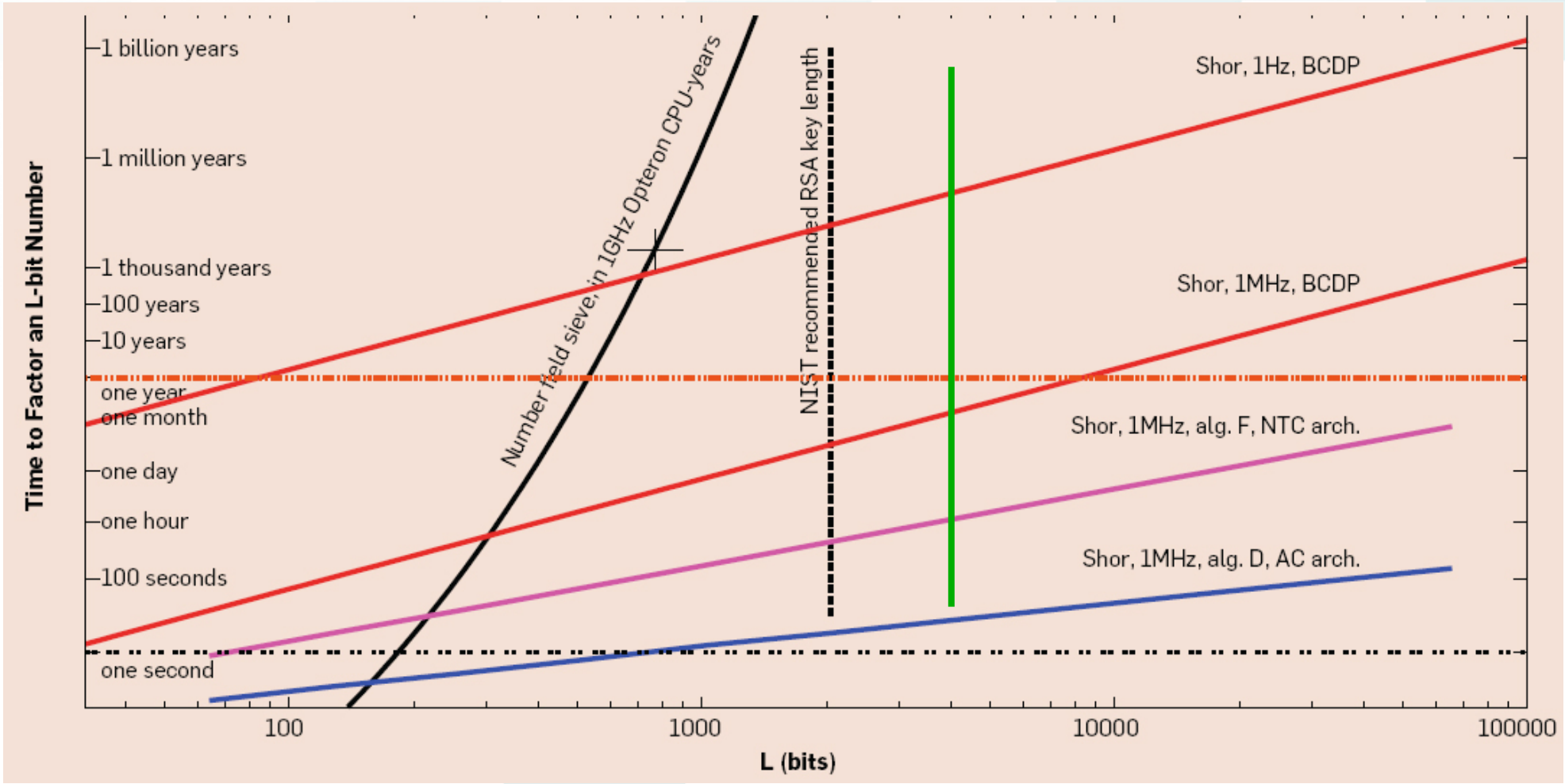
Quantum Computing - Auswirkungen

- Shor
  - DLP: Diffie-Hellman, ElGamal, ECC(ECDH, ECDSA)
  - Faktorisierung: RSA
  - × Alle asymmetrischen Verfahren lassen sich bei einer geeigneten Anzahl Qubits mit Shor's Algorithmus brechen.
- Grover
  - DES, AES
  - SHA1, SHA2, SHA3
  - × Grovers Algorithmus kann das brechen von symmetrische Kryptographie und von Hashfunktionen beschleunigen ($\sqrt{n}$).

Quantum Computing - Auswirkungen

- Asymmetrische Kryptographie
  - Diffie-Hellman, RSA, ElGamal (DSA), ECC (ECDH, ECDSA)
- Symmetrische Kryptographie
  - DES, AES256
- Kryptographische Hashfunktionen
  - SHA1, SHA2, SHA3

Quantum Computing - Auswirkungen

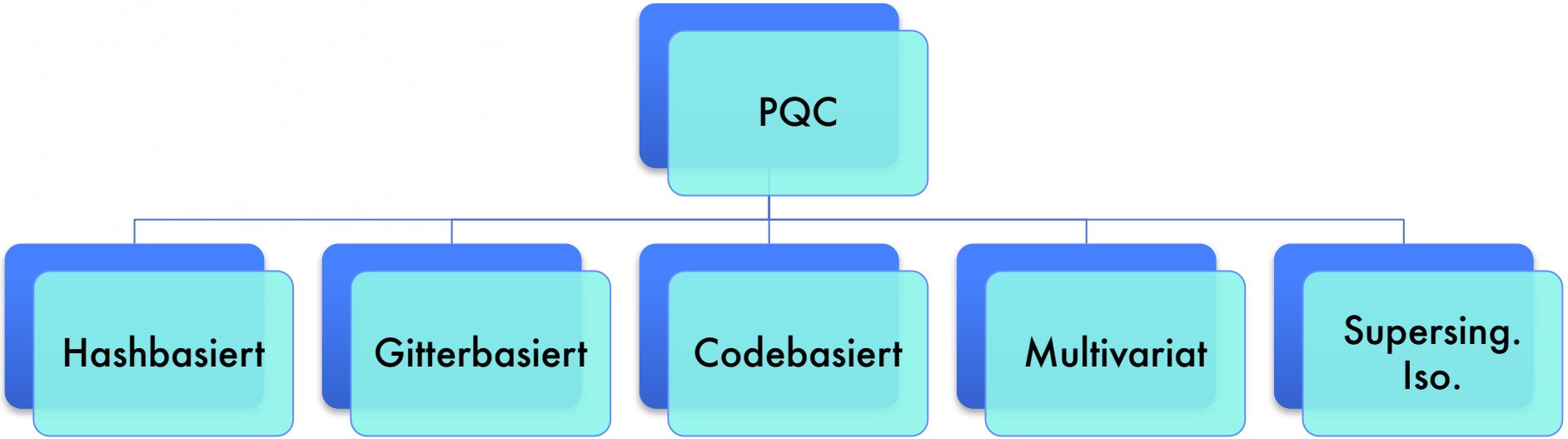


2L^2 = 8.388.608 logischen Quantenbits

BOREUS
rechenzentrum gmbh

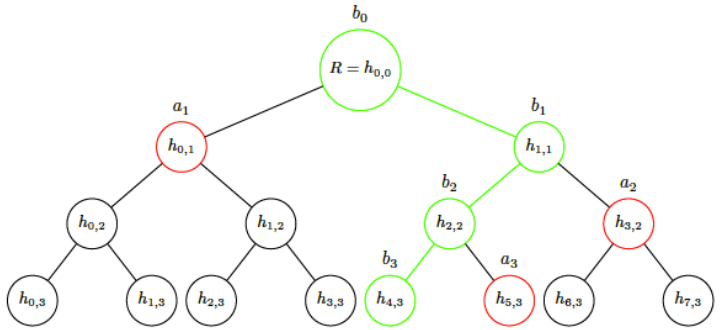
Post-Quanten-Kryptographie

Post-Quanten-Kryptographie - Verfahren



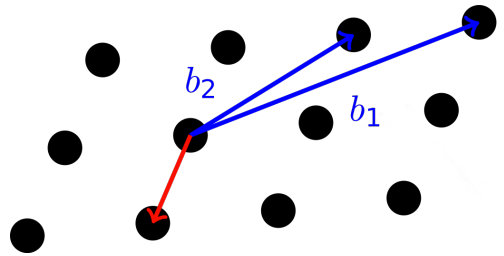
Post-Quanten-Kryptographie - Verfahren

- Hashbasierte Verfahren
  - Setzen auf die Sicherheit von Hashfunktionen
  - Neue Varianten durch Verwendung anderer Hashfunktionen möglich
  - Vertreter: Lamport-Diffie-OTS (1979), Merkle Signature Scheme (1970), eXtended MSS
  - LD-OTS muss ständig neue öffentliche Schlüssel versenden
  - MSS Signierschlüssel zu lang (2^H) Einmal-Sianierschlüssel



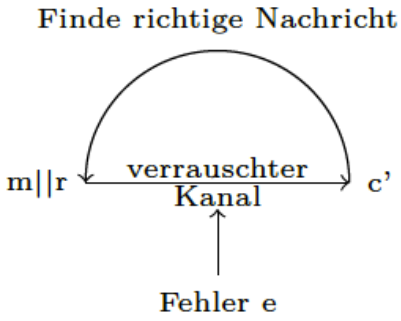
Post-Quanten-Kryptographie - Verfahren

- Gitterbasierte Verfahren
  - Setzen auf Gitterprobleme (z.B. SVP, CVP, (R-)LWE)
  - Finden schwerer Instanzen einiger Probleme schwer (Ajtai)
  - Schnelle Berechnungen bei hoher Sicherheit
  - Vertreter: Goldreich-Goldwasser-Halevi (1997), Lyubashevsky-Micciancio-OTS (2008), NTRU, BCNS (2015), NewHope (2015), MSR CLN16 (2016), Frodo (Okt. 2016)
  - Starke Forschung in diesem Bereich



Post-Quanten-Kryptographie - Verfahren

- Codebasierte Verfahren
  - Setzen auf fehlerkorrigierende Codes
  - Kodierungstheorie ist schnell, einfach zu implementieren
  - Vertreter: McEliece (1978), Niederreiter (1986), CFS (2001), Stern-IS (1993)
  - Extrem große Public Keys (4MBit (500kB) = RSA2048)
  - Aktive Forschung an der Schlüsselreduzierung
  - Geeignet für eingebettete System



Post-Quanten-Kryptographie - Verfahren

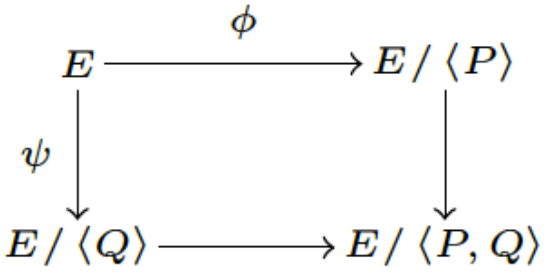
- Multivariate Verfahren
  - Setzen auf das Multivariate Quadratic ($\mathcal{MQ}$) Problem und das Isomorphism of Polynomials Problem (IP Problem)
  - Vertreter: Matsumoto-Imai (1988), Hidden Field Equations (1996)
  - hohes Sicherheitsicherheitsniveau
  - sehr schnell in der Verschlüsselung
  - Signaturen mit geringer Größe (HFE)
  - Wurden mehrfach gebrochen, HFE hat große Public Keys (100kB)

$$\mathbb{F}_q^n \xrightarrow{S} \mathbb{F}_q^n \xrightarrow{Q} \mathbb{F}_q^m \xrightarrow{T} \mathbb{F}_q^m$$

$$\underline{w} \mapsto \underline{x} \mapsto \underline{y} \mapsto \underline{z}$$

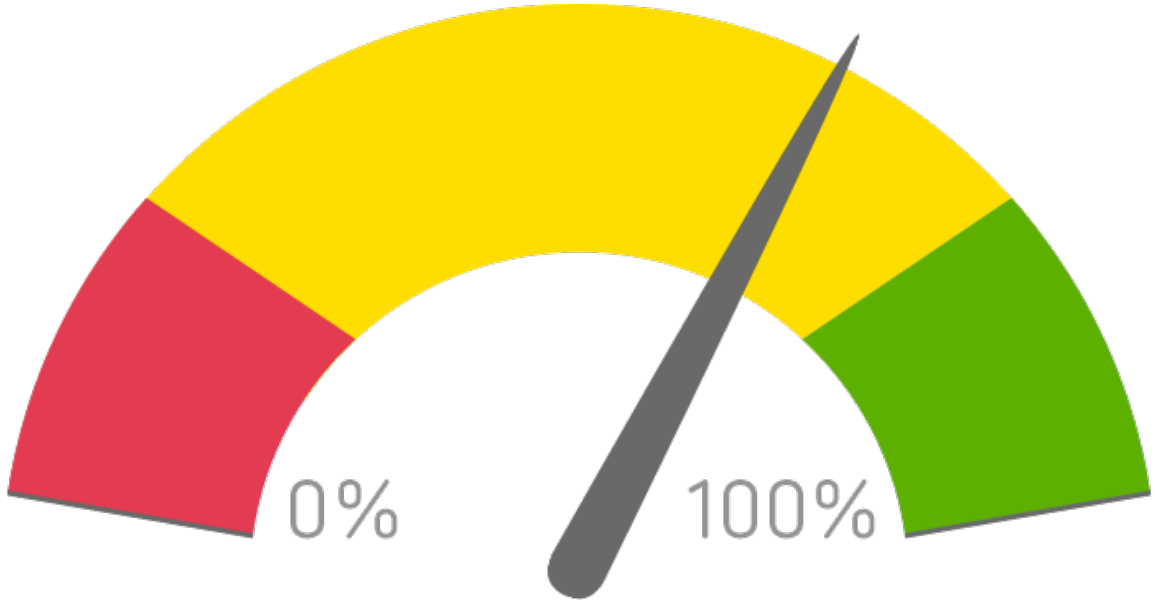
Post-Quanten-Kryptographie - Verfahren

- Verfahren auf supersingulären Isogenien
  - Setzen auf das Finden eines Weges, der zwei gegebene Vertices in einem Graphen aus supersingulären Isogenien, verbindet
  - Schlüssel sind größer als bei ECC, aber kleiner als bei RSA
  - Vertreter: Diffie-Hellman auf supersingulären Isogenien (SIDH, 2011)
  - SIDH stellt bisher Grundlage für Kryptofamilie dar



Post-Quanten-Kryptographie

Leistung



Post-Quanten-Kryptographie - Leistung

- Parameter der Leistungstests
  - 2 virtuelle Maschinen
  - 2 Intel Xeon E5 GHz vCPUs @ 2,53 GHz & 4 GB RAM
  - Debian 8.7 mit gcc 4.9.2 und OpenSSL 1.0.2k-dev (OQS)
- Leistungstest eigenständiger kryptographischer Operationen (OpenSSL speed)
- Leistungstest HTTPS-Verbindungen
  - Handshake-Latenz und -Größe, Verbindungsdurchsatz
- 500 durchgeführte Iterationen

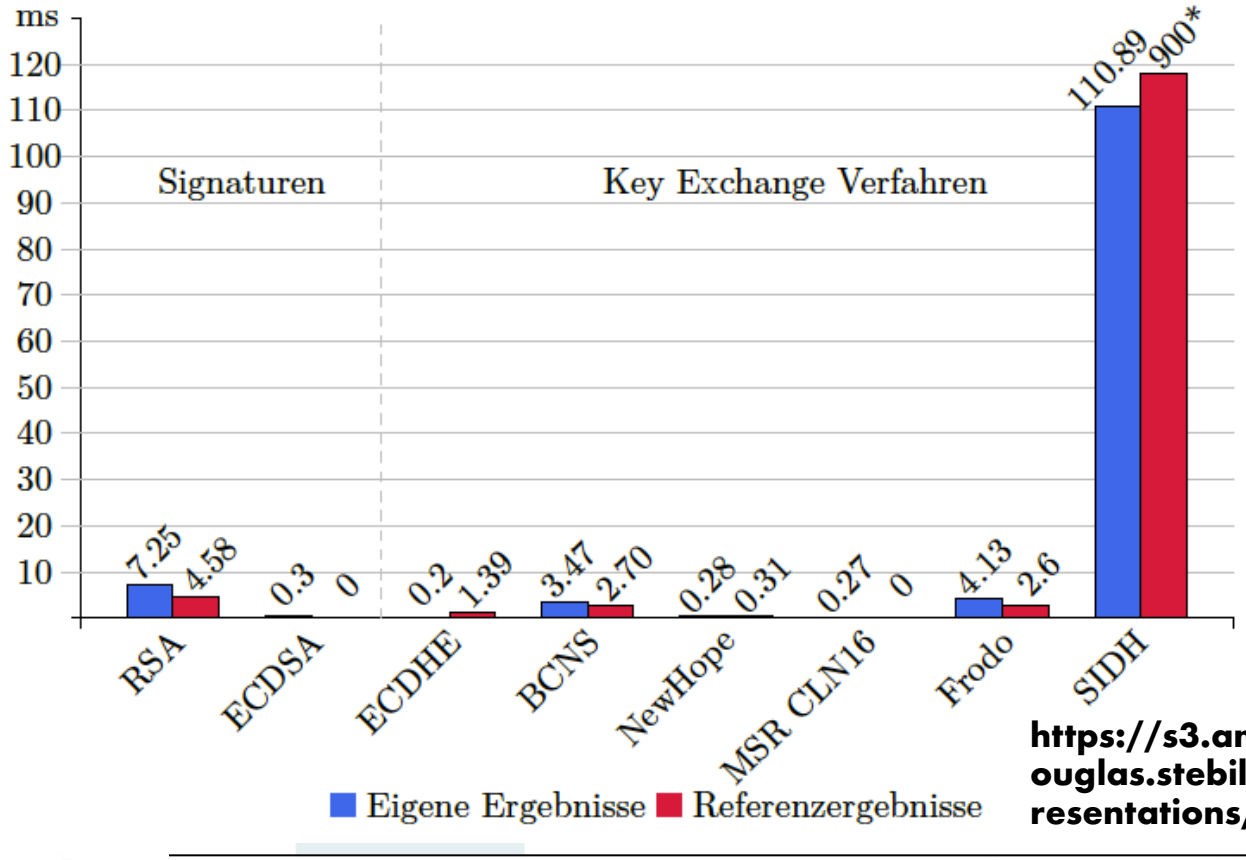
Post-Quanten-Kryptographie - Leistung

Sicherheitsniveaus der Testchiffren

Chiffre	Klassische Sicherheit	Quanten-sicherheit
RSA3072	128	-
ECDSA (nistp256)	128	-
ECDHE (nistp256)	128	-
BCNS	163	76
NewHope	229	206
MSR CLN16	229	206
Frodo Recommended	144	130
SIDH	192	128

Post-Quanten-Kryptographie - Leistung

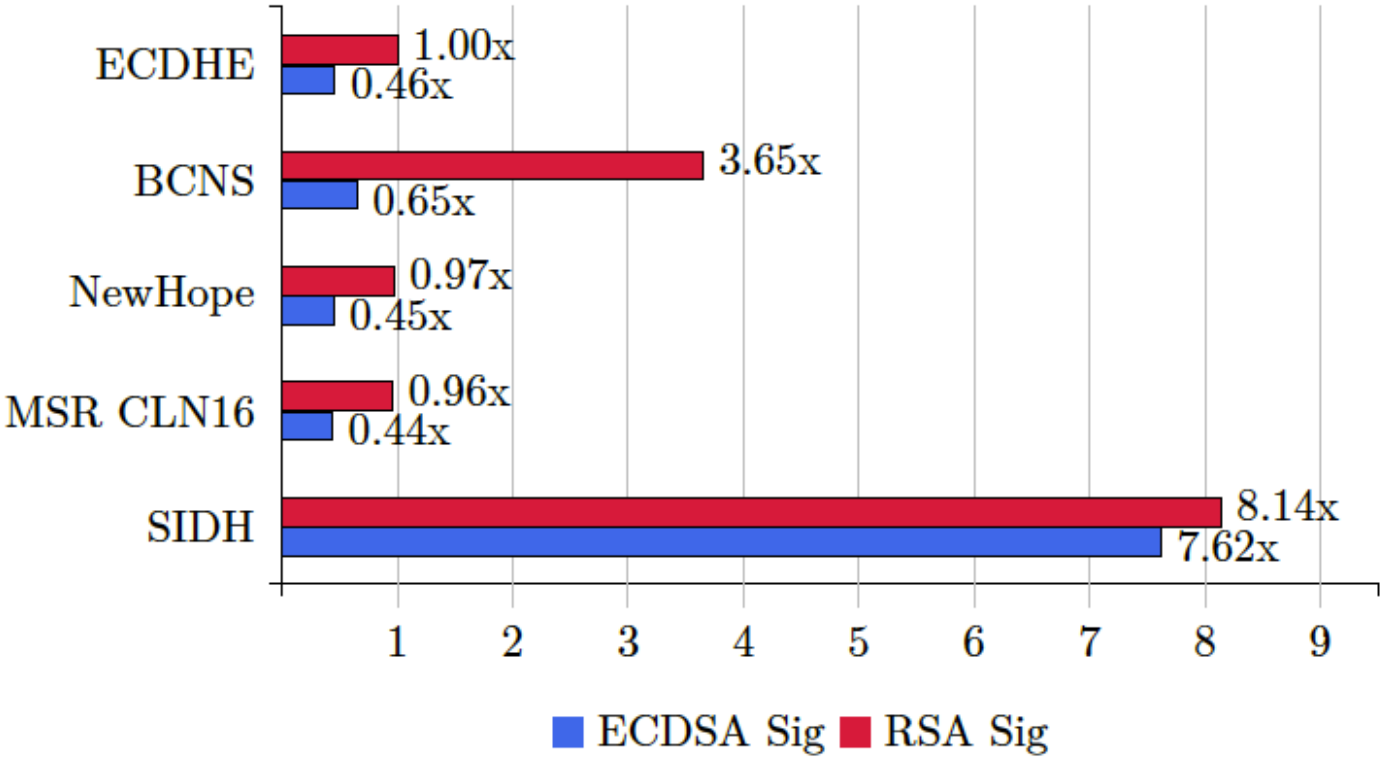
Leistungsfähigkeit (Standalone)



https://s3.amazonaws.com/files.douglas.stebila.ca/files/research/presentations/20160921-ETSI.pdf

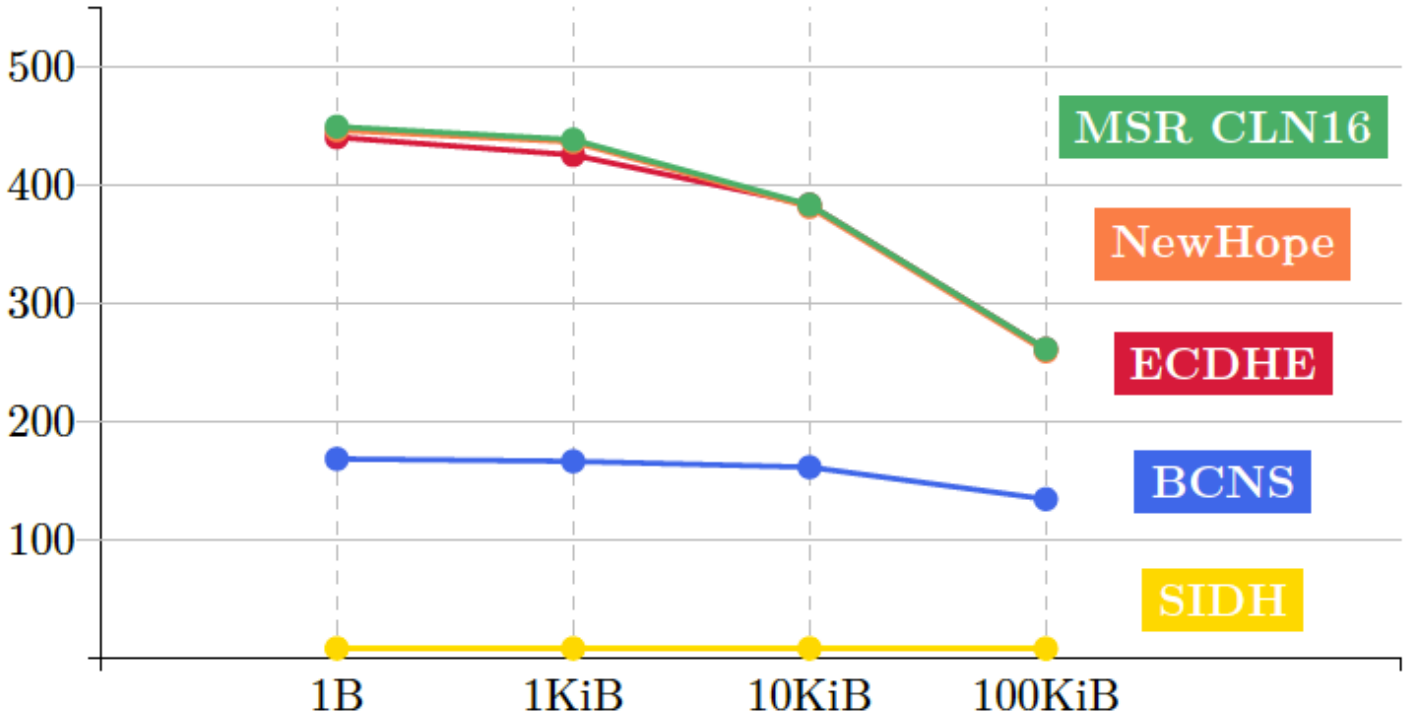
Post-Quanten-Kryptographie - Leistung

Leistungsfähigkeit (TLS Handshake-Latenz)



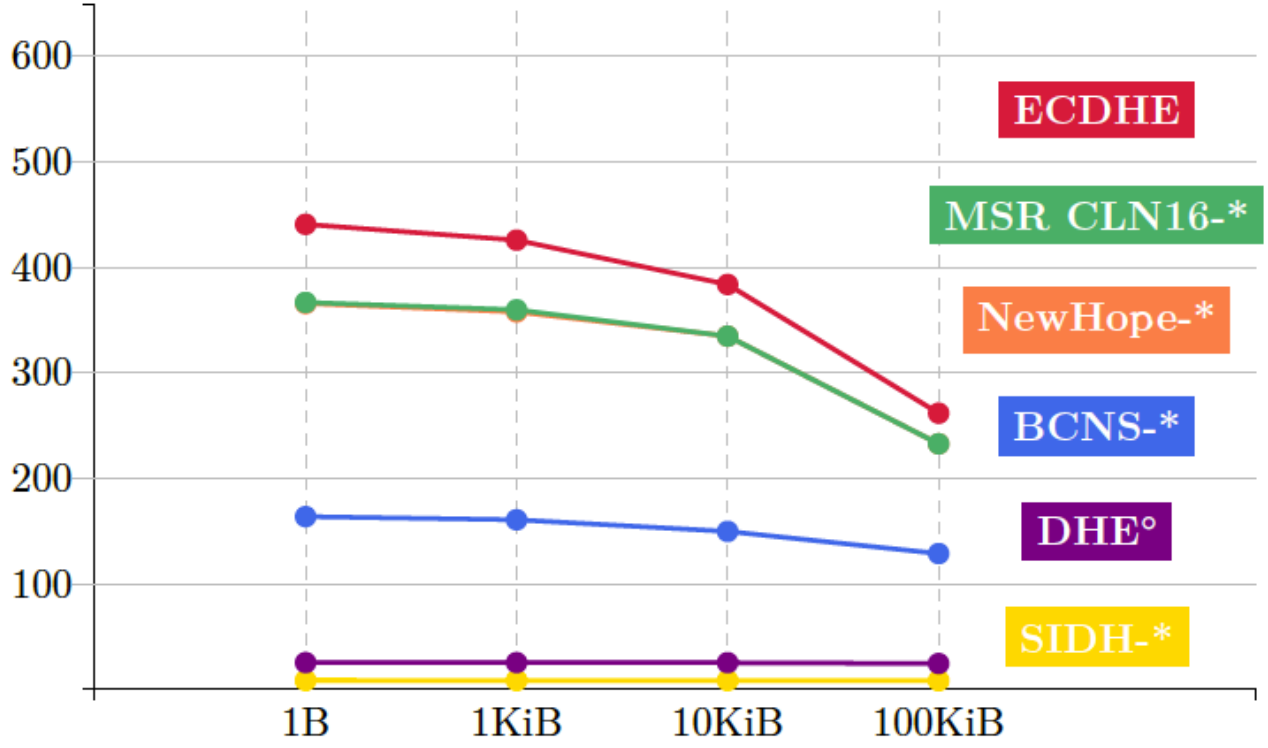
Post-Quanten-Kryptographie - Leistung

Leistungsfähigkeit (HTTPS-Con./Sekunde)



Post-Quanten-Kryptographie - Leistung

Leistungsfähigkeit (HTTPS-Con./Sekunde)

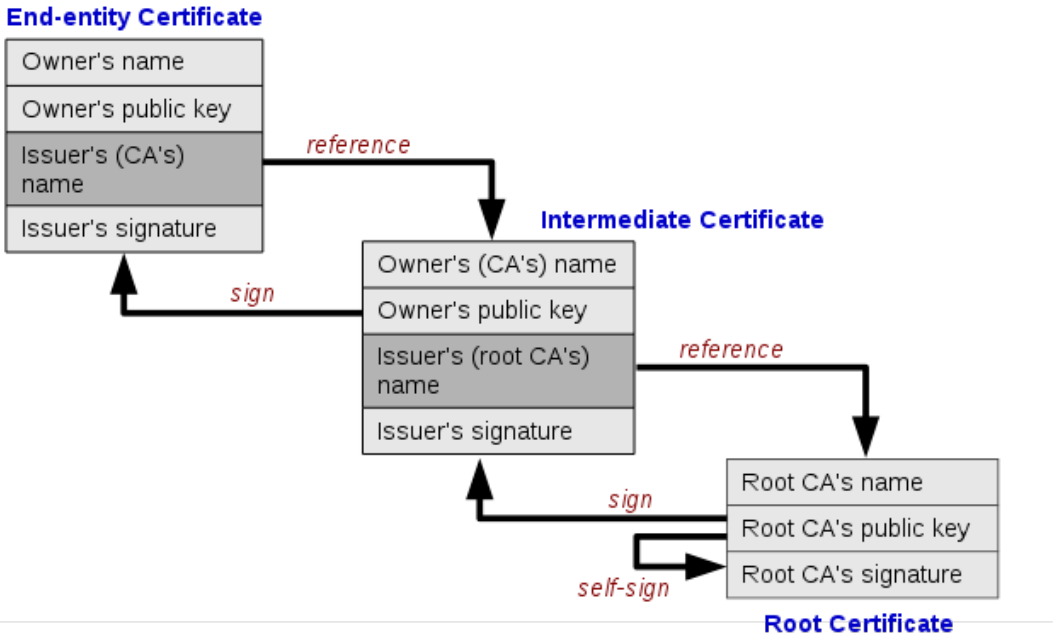


*OQSKEX mit ECDHE ° DH mit DSS

Bedeutung für heutige Rechnernetze

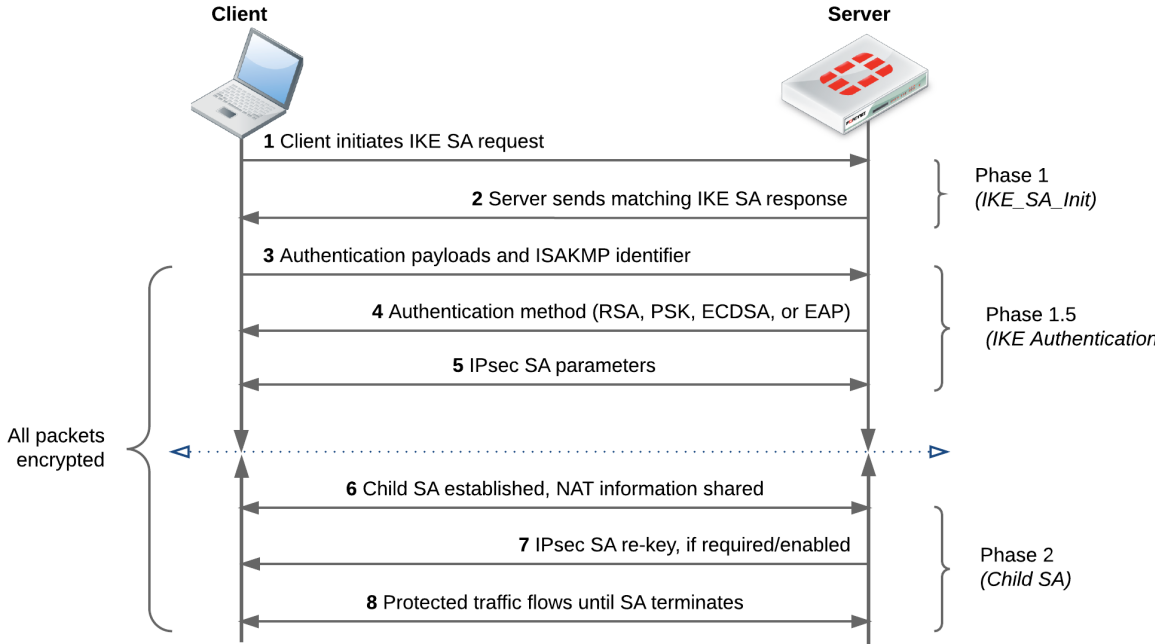
Auswirkungen auf heutige Netze

- X.509 Zertifikate
  - Bisherige Verfahren durch PQC-Verfahren austauschen (RSA)
  - "Chain of Trust": Root-Zertifikate (20 Jahre) und die damit generierten Zertifikate müssen ausgetauscht werden



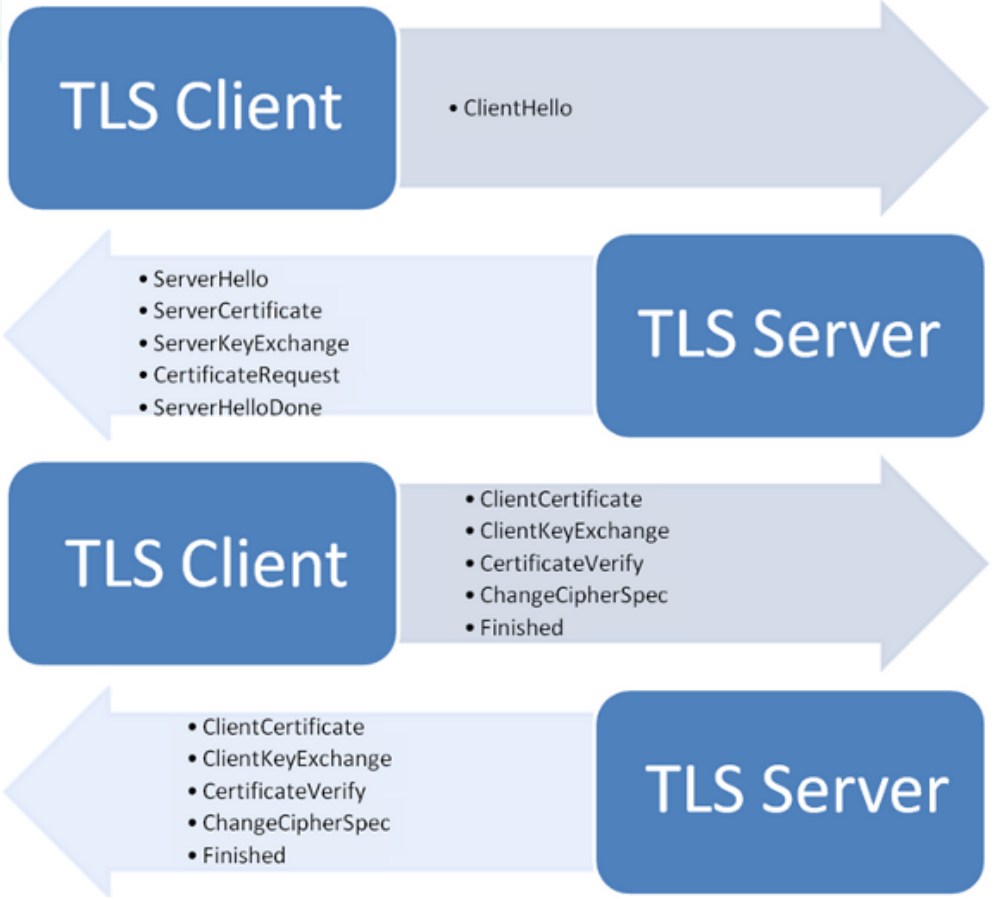
Auswirkungen auf heutige Netze

- Internet Key Exchange Version 2 (IKEv2)
  - Protokolländerung 1. und 3. Austausch (IKE_SA_INIT und CREATE_CHILD_SA): Diffie-Hellman muss durch PQC-Verfahren mit PFS ersetzt werden
  - Protokolländerung 2. Austausch (IKE_AUTH): RSA/DSA durch PQC-Signaturverfahren ersetzen



Auswirkungen auf heutige Netze

- Transport Layer Security
  - Ab TLS 1.3 nur noch authentifizierte Verfahren
  - Austausch der KEX-Verfahren
  - Austausch Signaturverfahren
  - Austausch restliche Verfahren



Auswirkungen auf heutige Netze

- S/MIME
  - Austausch der Signaturverfahren (DSA, RSA)
  - Austausch der symmetrischen Verfahren (AES)

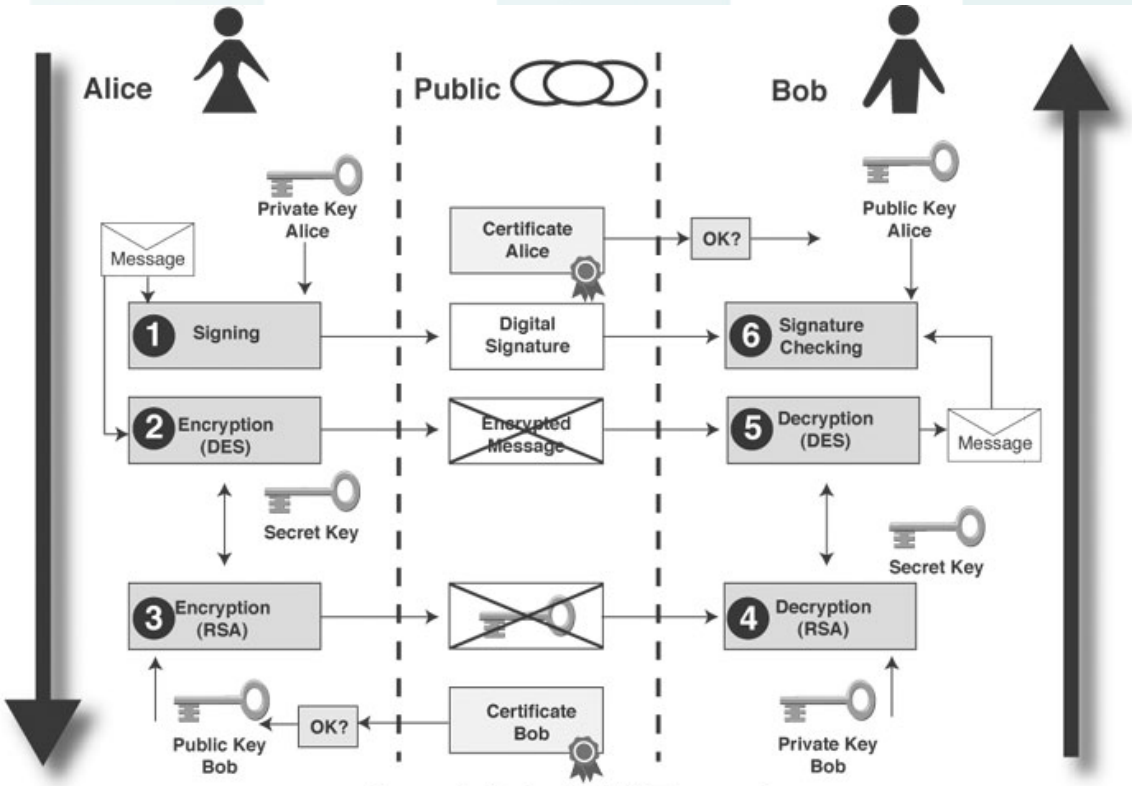
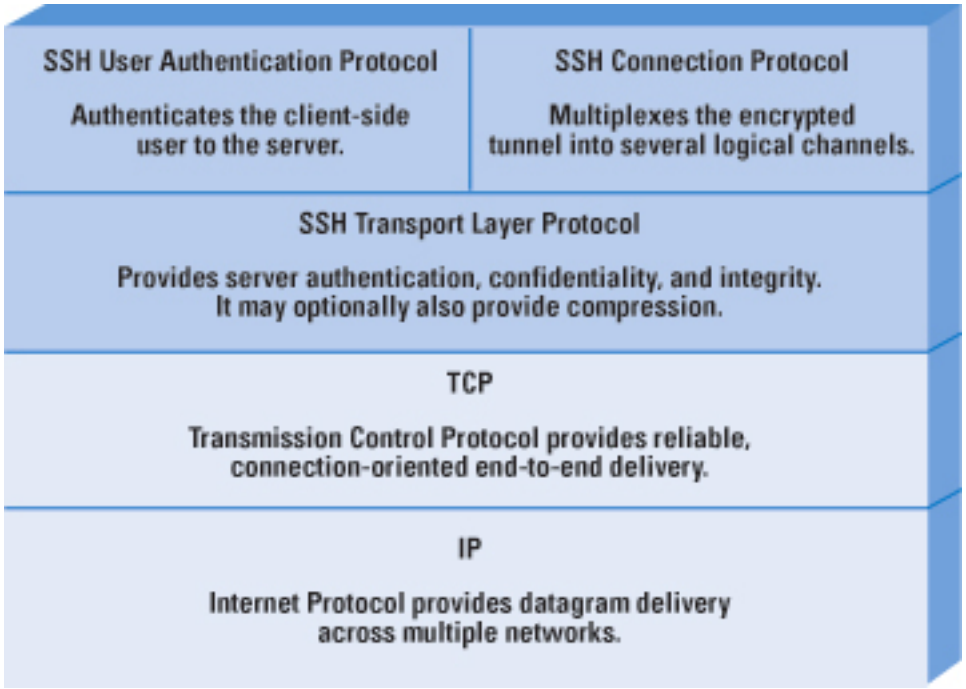


Figure 1: Typical S/MIME scenario

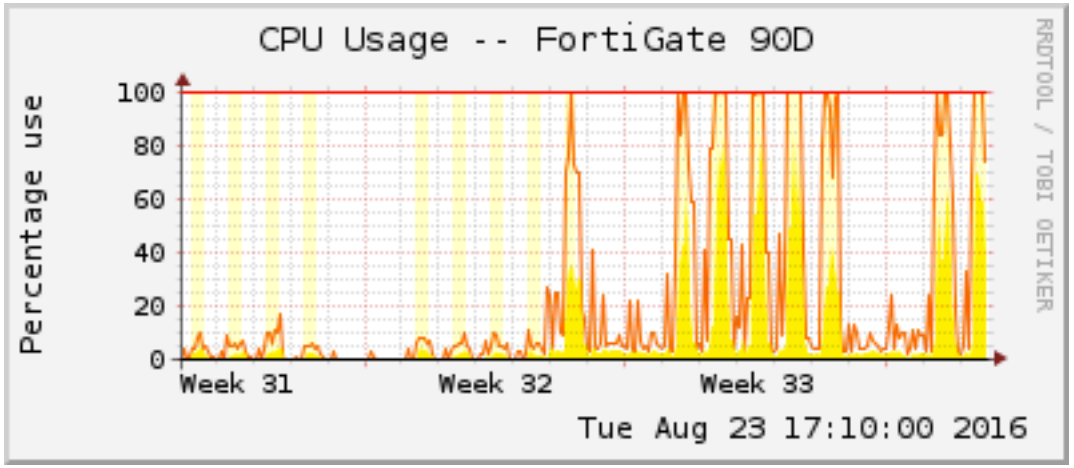
Auswirkungen auf heutige Netze

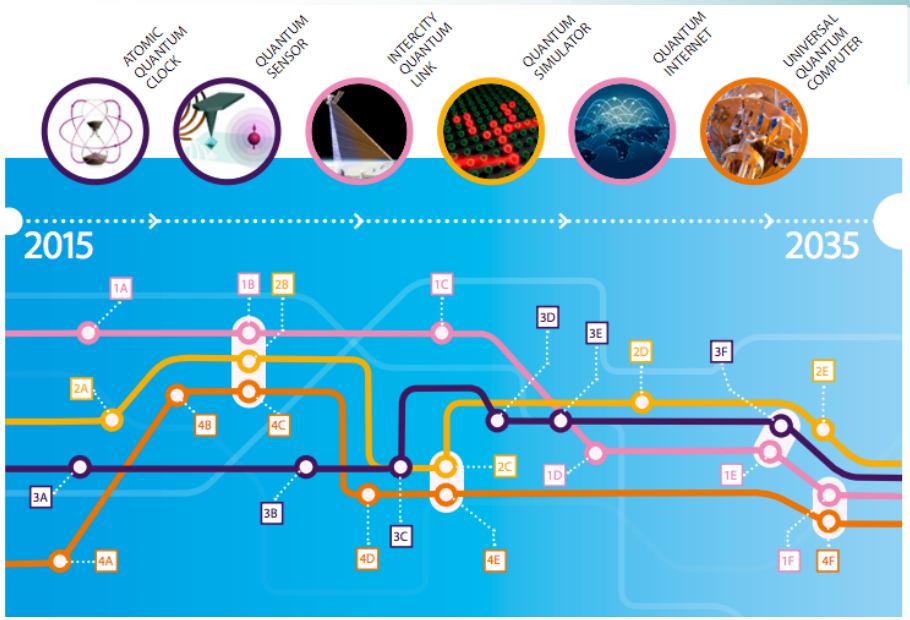
- Secure Shell Version 2 (SSH)
  - Austausch der KEX-Verfahren (DH)
  - Austausch Signaturverfahren (RSA, DSA, ECDSA)
  - Austausch restliche Verfahren (AES)



Auswirkungen auf heutige Netze

- Weitere Auswirkungen
  - Mehr Last auf CPU und Netzwerk durch höhere Schlüsselstärken und größere Schlüssel
  - AES mit 256Bit und SHA* mit 256Bit Ausgabelänge





Ein kleiner Ausblick

Ausblick und Fazit

- EU Quantum Manifesto (1 Milliarde)
  - EU wettbewerbsfähig machen
  - Bis 2035 universeller Quantencomputer
- Standardisierung PQC durch die NIST bis spätestens 2025
  - Sammeln und auswählen mehrerer geeigneter Verfahren
  - Verfahren können bis 30.11.2017 eingereicht werden
- Standardisierung von XMSS (TU Darmstadt)
- Quantencomputer Blueprint (golem.de)
- Univ. QC frühestens ab 2030

BOREUS
rechenzentrum gmbh

Vielen Dank für die Aufmerksamkeit
Für Fragen stehe ich nun zur Verfügung

BOREUS rechenzentrum gmbh

Quellen

- https://de.wikipedia.org/wiki/Datei:Schrodingers_cat.svg
- https://saimg-a.akamaihd.net/saatchi/395191/art/1626680/821923-8.jpg
- http://www.spektrum.de/lexikon/physik/bracket-notation/1926
- https://commons.wikimedia.org/wiki/File:Dirac_4.jpg
- http://abyss.uoregon.edu/~js/images/qc4.jpg
- https://volksbetrugpunktnet.files.wordpress.com/2014/01/1e33a-quantumcomputer.jpg
- https://www.mpq.mpg.de/4882546/11_05_26
- https://de.wikipedia.org/wiki/Datei:Schroedingers_cat_film.svg
- https://commons.wikimedia.org/wiki/File:Ionenfalle_-_Quantencomputer.jpg
- https://www.computerbase.de/bildstrecke/72101/4/
- https://commons.wikimedia.org/wiki/File:BQP_complexity_class_diagram.svg

BOREUS rechenzentrum gmbh

Quellen

- https://www.sciencenews.org/sites/default/files/2017/04/main/articles/041817_TS_asteroid_main_FREE.jpg
- https://www.contra-magazin.com/wp-content/uploads/2016/01/Atombombe-620x330.jpg
- https://commons.wikimedia.org/wiki/File:SVP.svg
- https://compass-blog.s3.amazonaws.com/uploads/2016/09/benchmark-hero.png
- https://commons.wikimedia.org/wiki/File:Chain_of_trust.svg
- http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/Images/IKEv2_process.png
- https://www.ibm.com/developerworks/webservices/library/ws-ssl-security/flow.png
- http://windowsitpro.com/site-files/windowsitpro.com/files/archive/windowsitpro.com/content/content/49878/figure_01.jpg

- https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-46/124-ssh.html
- https://blog.webernetz.net/wp-content/uploads/2016/08/CPU-Usage-FortiGate-100D-90D-featured-image.png
- http://www.weltderphysik.de/gebiet/technik/news/2017/der-rest-ist-ingenieursarbeit/

Literaturempfehlungen

- Matthias Homeister. Quantum Computing verstehen. Grundlagen - Anwendungen - Perspektiven.
- http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
- http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf